View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Missouri University of Science and Technology (Missouri S&T): Scholars' Mine

Missouri S&T's Peer to Peer

Volume 1 | Issue 1 Article 3

February 2016

The Implications of RFID Technology in University ID Cards

Michael Beaver

Follow this and additional works at: https://scholarsmine.mst.edu/peer2peer

 Part of the Information Security Commons

Recommended Citation

Beaver, Michael. 2016. "The Implications of RFID Technology in University ID Cards." *Missouri S&T's Peer to Peer* 1, (1). https://scholarsmine.mst.edu/peer2peer/vol1/iss1/3

This Article - Journal is brought to you for free and open access by Scholars' Mine. It has been accepted for inclusion in Missouri S&T's Peer to Peer by an authorized administrator of Scholars' Mine. This work is protected by U. S. Copyright Law. Unauthorized use including reproduction for redistribution requires the permission of the copyright holder. For more information, please contact scholarsmine@mst.edu.

The Implications of RFID Technology in University ID Cards

Michael Beaver
Missouri University of Science and Technology

Radio frequency identification (RFID) chips have been rising in popularity because of their usefulness and convenience, and have now made their way into the ID cards of universities. An RFID chip is an identification device that, when powered by some nearby source, sends out a signal with information that was stored in the chip. RFID physical security systems work just like a lock and key, with the RFID chip acting as the key. Instead of having a unique pattern, RFID chips have an identification code that is read by the lock. Some RFID chips also hide this code behind a series of encryptions. While this can be very convenient when used for door locks and quick pay systems, there are still many RFID chips that have insufficient securities protecting the information they hold. Based on the increasing trend of RFID usage (RFID forecasts, 2014), it is safe to assume that many more universities will follow. However, this convenience could come at the cost of security. The implementation of RFID technology in ID cards on college campuses could be a serious security risk if universities do not commit to ongoing investments in security and research.

RFID Insecurities

Northern Arizona University (NAU) is one example of an innovative university that is utilizing RFID chips in their student ID cards. This system has allowed professors to record student attendance automatically, which became relevant once "student attendance (and attendance collection by

instructors) became mandatory"(NAU, 2013) in 2012. NAU made this policy because "Numerous studies show a strong correlation between attendance and student success" (NAU, 2013) and they have seen great results. Even though there are considerable benefits to using RFID chips in student ID cards, some argue that they shouldn't be used for students at all. They believe that the RFID chips provide an unacceptable form of tracking on the students that amounts to a breach of student privacy. There are even "three Texas bills [that] seek to either curtail or outright ban the use of RFID student trackers" (Barnes, 2013). The issue here is whether or not RFID technology is too much of a loose cannon for use in student ID cards because while there are very significant benefits, there certainly are risks involved that need to addressed.

In 2013, Francis Brown spoke at a hacking conference about how he successfully accessed an RFID physical security system. He accomplished this by discreetly stealing access information from the RFID chips in employee entry devices. He then took this information and created a card clone, which he used to grant himself access to restricted areas protected by the RFID security systems (Brown, 2013). Brown has made all of the information that he used and created for this project available online. These resources provide all the tools necessary for anyone to discreetly steal information from RFID chips.

Chris Paget's research was completely devoted to reading RFID chips from as far away as possible. This involved the use of EPC Gen 2 RFID chips which are significantly different from most chips. EPC Gen 2 "supports operation at long distances (e.g., 25-30 feet), and has minimal support for security" (Smart Card Alliance, 2006). These chips can be found in various applications such as U.S. passports, enhanced drivers licenses, and even "leading organizations, such as the U.S. Department of Defense and Wal-Mart, have set goals for their suppliers to begin using RFID on shipments to their organizations" (Saygin & Sarangapani, 2007). Paget was capable of reading these chips from over 200 feet away, and he believes that longer ranges are possible (Paget, 2010).

There are a number of possible consequences to malicious persons being capable of collecting

information from RFID systems discreetly and illicitly. Someone could grant themselves access to restricted areas, leading to anything from stealing information to obtaining restricted chemicals, the ramifications of which could be severe. At the same time, someone could also steal financial and personal information and use it to make purchases with the victim's money. Beyond theft, there are a number of other issues that could arise. If using EPC Gen 2 chips someone could stalk an individual from over 200 feet away, and thereby determine a student's daily schedule, and even identify when there are no other students nearby. These are just a few examples though, crimes are always changing and becoming more complex, and the versatility of RFID chips will only aid that development.

University Security

Although not every university has implemented RFID technology, it has been continuously increasing, and this trend is expected to continue. In 2014 the market worth of RFID technology was "$9.2 billion" and "IDTechEx forecast that to rise to $30.24 billion in 2024" (RFID forecasts, 2014). Based on this, it should be safe to assume that most universities will eventually implement some form of RFID system. When this happens, it is important that universities continually invest in the security of their RFID systems. When a university is implementing RFID technology, an investment into both security and research needs to be made to ensure the safety of its students. A large initial investment into determining what technology is secure and appropriate for the university is necessary to avoid preliminary mistakes that could create a very insecure system. This is not where the investment ends though. The university needs to be continuously researching the security of their system to stay ahead of hackers and other criminals with malicious intent.

One university that has begun implementing RFID technology in their ID cards is the Missouri University of Science & Technology (S&T). In an interview, Karl Lutzen, the Chief Information Security Officer at S&T, noted that when the university was selecting a chip to use, security was a major concern.

This is important because he indicated that, starting in 2015, S&T is planning on implementing an RFID physical security system in the form of electronic door locks (personal communication, April 4, 2015). He also stated that S&T ID cards house a "MIFARE DESFire EV1 Smart Card" which is "compliant to all 4 levels of ISO/IEC 14443A[1]" (MIFARE, 2013) and uses a "3DES hardware cryptographic engine for enciphering transmission data" (MIFARE, 2013). Triple DES, abbreviated as 3DES, is an encryption method that is derived from an older method known as DES. 3DES applies the DES algorithm in triplicate in order to create a more secure system. As of the date of this article, there is no known or publicized way to break the 3DES encryption. While this system does appear to be very secure there are still some possible lapses in protection. For example, Gerhard P. Hancke's (2006) research examines practical attacks on ISO 14443 RFID systems and he discusses that he was able to complete a successful relay attack on this type of proximity card. There are also some unsafe procedures being practiced at S&T with student ID cards. Lutzen expressed immediate concern when he was told that the front desks of residential halls require ID cards as collateral for rentals, which could provide access to each student's account information if a competent hacker was able to acquire them. Because of these concerns, S&T has students that will be conducting research with a professor on the RFID system in the 2015-2016 academic year in order to guarantee the security of the students at S&T.

RFID with Caution

RFID technology certainly has a place in university ID cards, but not without the ongoing investment by universities into security and research. When implementing an RFID system, universities should look for a suitable RFID chip to use. When researching RFID chips, it is encouraged that a high

[1] ISO stands for the International Organization for Standardization, and they are "an independent, non-governmental membership organization" that gives "world-class specifications for products, services and systems, to ensure quality, safety and efficiency" (ISO, 2015). ISO 14443A is a classification that defines proximity cards used for identification, and the transmission protocols for communicating with it (ISO, 2008).

level encryption be a top priority. While it might be tempting to find a chip that is inexpensive, this is not an area to cut costs. If a university feels it needs to cut back on how much it spends on an RFID system, then it is likely not ready and should instead wait until it can afford to implement the system properly. Once in place, the RFID system needs to be maintained. This maintenance involves more than just routine procedures to keep the system running. It also involves continuously researching potential faults in the security of the RFID system. It is recommended to have this task either delegated to several employees who convene semi-regularly to discuss any possible security breaches, or to create a specific position with this research as a primary assignment. Some situations may arise where the system seems secure at face value, but there is some emerging research suggesting some potential exploits. In this situation, a university would likely be hesitant to hastily spend more money on the system, but universities shouldn't be afraid to follow the lead of S&T and allow some undergraduate students the opportunity to perform their own research with a professor to investigate the issue. This approach has the potential to solve the problem right away, and even if it is unsuccessful, it still would provide experiential learning for the students involved. Achieving this level of investment, as is currently being done at S&T, is crucial to securely implementing an RFID system. Any university looking to utilize RFID technology should ensure it can commit to this kind of ongoing investment into both security and research.

References

Brown, Francis. (2013). Live Free or RFID Hard [Presentation]. In *DEF CON*, Retrieved from https://www.defcon.org/html/links/dc-archives/dc-21-archive.html

Barnes K. (2013, May 3). *CPW 2013: When FERPA Fails to Make the Grade, States Ratchet up Student Privacy Laws*. Retrieved from https://chooseprivacyweek.org/when-ferpa-fails-to-make-the-grade-states-ratchet-up-student-privacy-laws/

Hackne, G.P. (May 21-24, 2006) Practical Attacks on Proximity Identification Systems *Security and Privacy, 2006 IEEE Symposium on*, 6-333. doi:10.1109/SP.2006.30

International Organization for Standardization. (2008). *ISO/IEC 1443-1:2008(en)*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-1:ed-2:v1:en

International Organization for Standardization. (2015). *About ISO*. Retrieved from http://www.iso.org/iso/home/about.htm

MIFARE (2013). *MIFARE DESFire EV1*, Retrieved from http://www.mifare.net/en/products/mifare-smartcard-ic-s/mifare-desfire-ev1/

Northern Arizona University. (2013, August 27). *What are Proximity Card Readers?*. Retrieved from http://www2.nau.edu/d-elearn/faq/keywords_134

Paget, Chris. (2010). Extreme-range RFID Tracking [Presentation]. In *DEF CON* Retrieved from https://www.defcon.org/html/links/dc-archives/dc-18-archive.html.

(2014, September). RFID Forecasts, Players and Opportunities 2014-2024. *RFID (Radio Frequency Identification) Newsletter, 11*(9).

Saygin, Can and Sarangapani, Jagannathan. (2007). RFID in manufacturing: the good, the bad, and the ugly. *Faculty Research & Creative Works*. Paper 8252.

Smart Card Alliance Identity Council. (2006, July). *Contactless Smart Cards vs. EPC Gen 2 RFID Tags: Frequently Asked Questions*. Retrieved from http://www.smartcardalliance.org/publications-epc-gen2-faq/#2